SEC-202: Secure Start-Up

Lecture 7 – The Human Element & Future Careers

"Security is a People Problem." Technology is just the tool; culture is the strategy.

Instructed By:

Dr. Charnon Pattiyanon

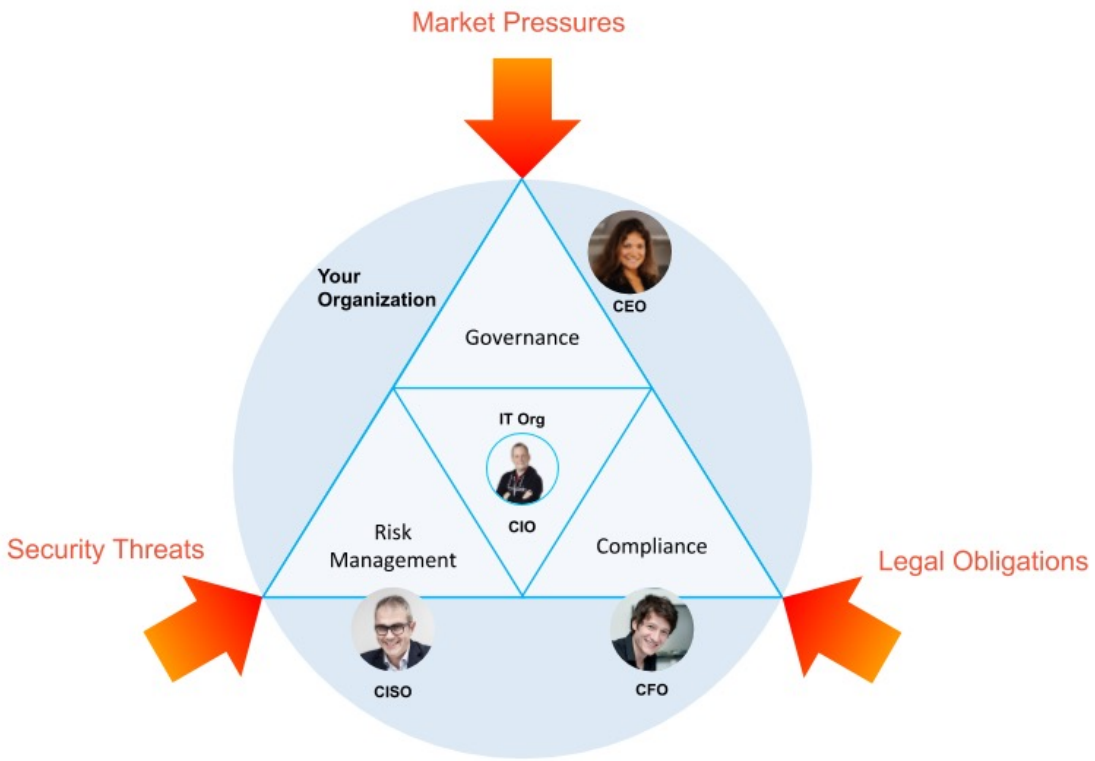
Assistant Director of IT and Instructor
CMKL University

Artificial Intelligence and Computer Engineering (AICE) Program

Today’s Outline

- Designing the Security Organization
- Security Culture
- Insider Threats
- Hiring and Retention
- Outsourcing Strategy
- Certification Roadmaps
- Networking and Community
- Ethics in Cybersecurity
- Future Trends

Designing the Security Organization



- **Reporting Lines:**
  - CISO -> CIO: Traditional.

    Risk: "Speed" (CIO) conflicts with "Safety" (CISO).
  - CISO -> CEO/CRO: Modern.

    Ensures independent risk oversight.
- **Functional Teams:**
  - GRC: Policy, Compliance, Risk.
  - SecOps (SOC): Monitoring, Incident Response.
  - Product Security: AppSec, DevSecOps.
  - Identity: IAM, Access Control.

The "Skills Gap" Myth

- **The Paradox:** 3 million unfilled jobs, yet juniors can't get hired.
- **The Problem:**
  - Job Descriptions asking for "Entry Level" with "CISSP + 5 years experience."
  - Over-reliance on degrees vs. practical skills.
- **The Solution:** Hire for aptitude and curiosity, then train the technical skills.

IT Security

View all jobs

Phaya Thai, Bangkok

Security (Information & Communication Technology)

Full time

Add expected salary to your profile for insights

Posted 2h ago

EDUCATION AND EXPERIENCE:

- 4–5+ years of experience in IT Security Management and project delivery in regulated/complex environments (banking, fintech, insurance, etc.).
- Bachelor’s degree in Computer Engineering, Computer Science, IT, or related field.

Security Culture

- **The "Department of No":**
  - If Security always says "No," employees will find a workaround (Shadow IT).
- **The Goal:** "Yes, but..." (The "Department of How").
- **Building Culture:**
  - Reward people for reporting phishing (don't just punish them for clicking).
  - Make security easy (UX matters).

Security Culture

Attitudes
The feelings and beliefs that employees have toward the security protocols and issues

Behaviours
The actions and activities of employees that have direct or indirect impact on the security of the organization

Cognition
Employees' understanding, knowledge, and awareness of security issues and activities

Communication
The quality of communication channels to discuss security-related topics, promote a sense of belonging, and provide support for security issues and incident reporting

Compliance
The knowledge of written security policies and the extent that employees follow them

Norms
The knowledge of and adherence to unwritten rules of conduct in the organization

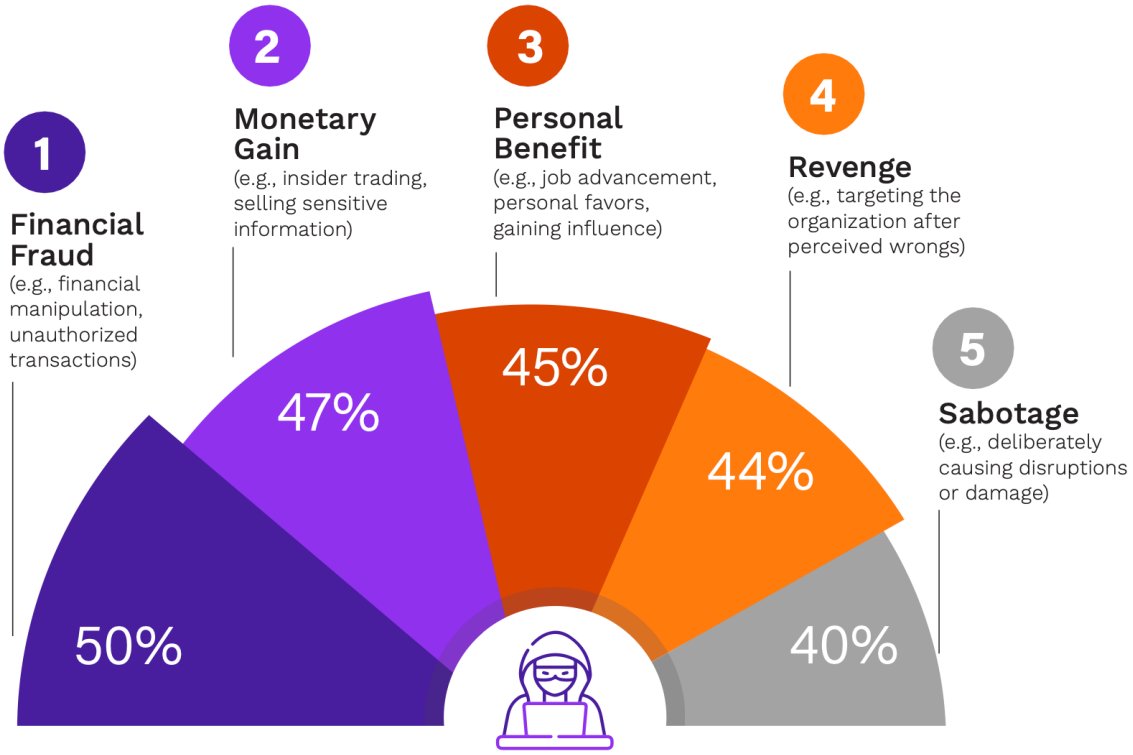
Responsibilities
How employees perceive their role as a critical factor in sustaining or endangering the security of the organization

Insider Threats

- **Types:**
  1. **Malicious Insider:** A disgruntled employee stealing IP before quitting.
  2. **Accidental Insider:** The "Click-Happy" employee (90% of cases).
  3. **Compromised Insider:** An employee whose credentials were stolen.
- **Controls:**
  - **DLP (Data Loss Prevention):** Detecting large file uploads to personal USBs/Cloud.
  - **Exit Procedures:** Revoking access immediately upon termination.

Insider Threats

What motivations behind malicious insider threats are you most concerned about?



Common indicators of an insider threat

Unusual Behavior
Sudden schedule changes, accesssing unusual files, irritability, or stepping out of job scope

Gaining Extra Access
Attempts to gain higher permissions or bypass controls not needed for role

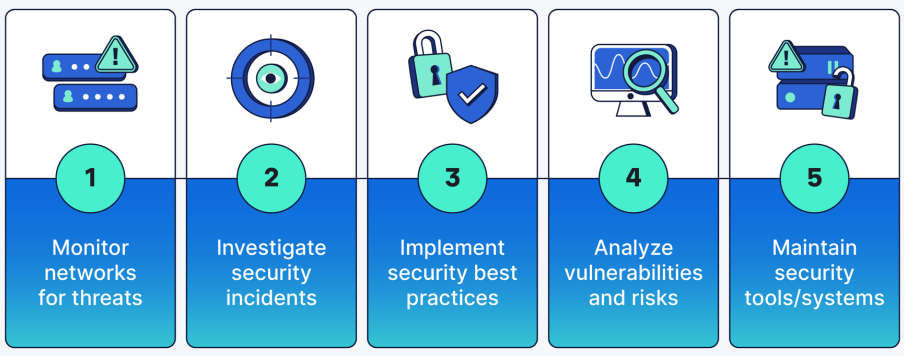
Suspicious Activity
Large data transfers, security tool tampering, or frequent confidential searches

Access Anomalies
Unusual logins from distant locations or unrecognized devices, use of dormant accounts

Data Theft Attempts
Large file transfers to personal storage or external entities—track and flag anomalies

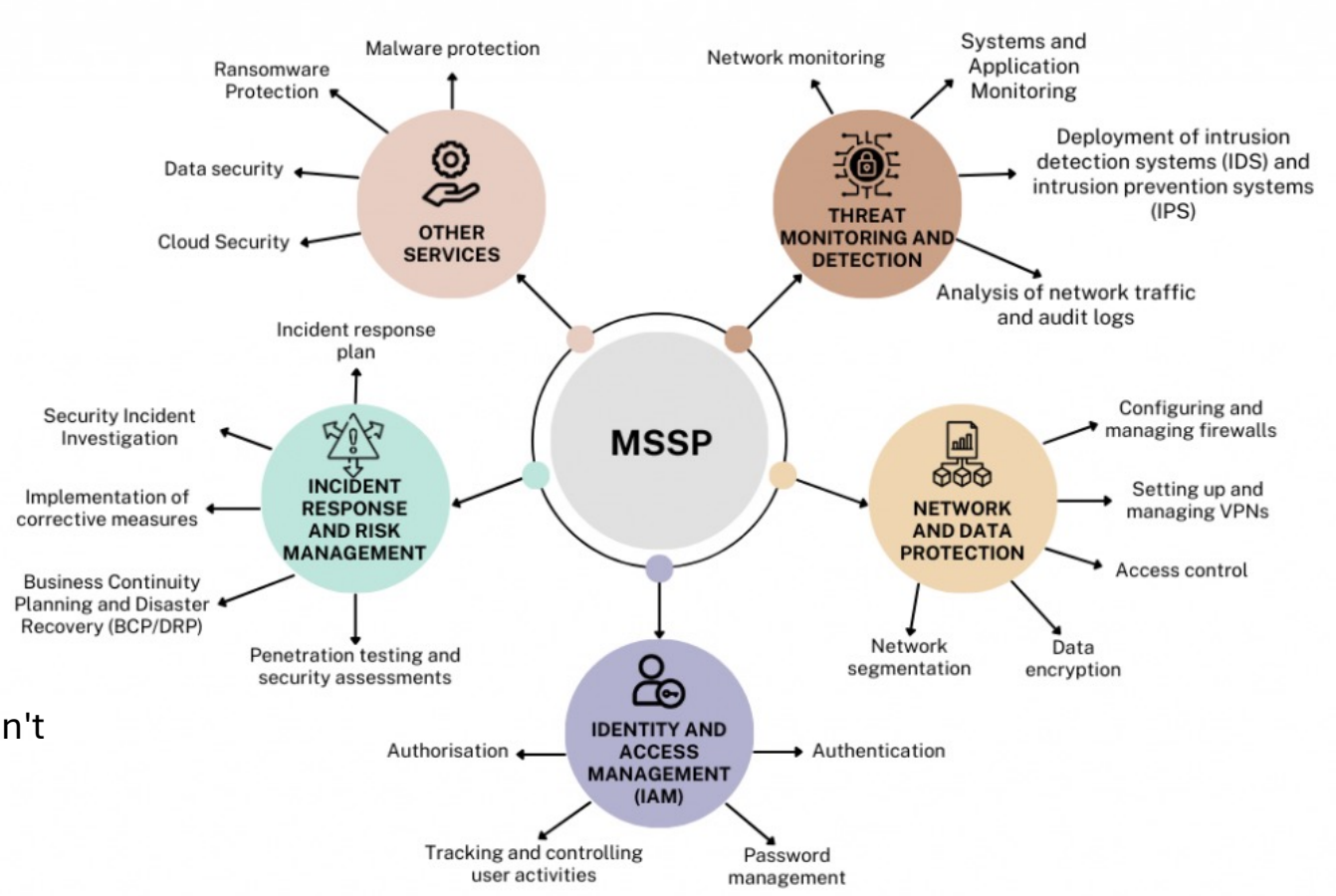
Hiring and Retention

- **Burnout:**
  - Security is a high-stress, 24/7 job.
  - Average CISO tenure is only 18-24 months.
- **Retention Strategies:**
  - **Rotation Programs:** Let a SOC analyst try Engineering for 3 months.
  - **Training Budget:** Pay for their certifications (SANS, OSCP).
  - **Blameless Culture:** Psychological safety is crucial.



Outsourcing Strategy

- **MSSP (Managed Security Service Provider):**
  - Outsourcing the "Eyes on Glass" (24/7 Monitoring).
- **vCISO (Virtual CISO):**
  - Hiring a fractional executive for strategy (Great for startups).
- **Pros:** Lower cost, 24/7 coverage.
- **Cons:** Lack of business context (They don't know *your* specific risks).



Certifications Roadmap

- **Entry Level:**
  - **Security+ (CompTIA):** The baseline.
  - **Network+:** You can't secure a network if you don't know how it works.
- **Management:**
  - **CISSP:** The "Gold Standard" for HR filters.
  - **CISM:** Focused on management/strategy.
- **Technical:**
  - **OSCP:** Hands-on hacking (Red Team).
  - **GCIH/GCFA (SANS):** Incident Response (Blue Team).

Networking and Community

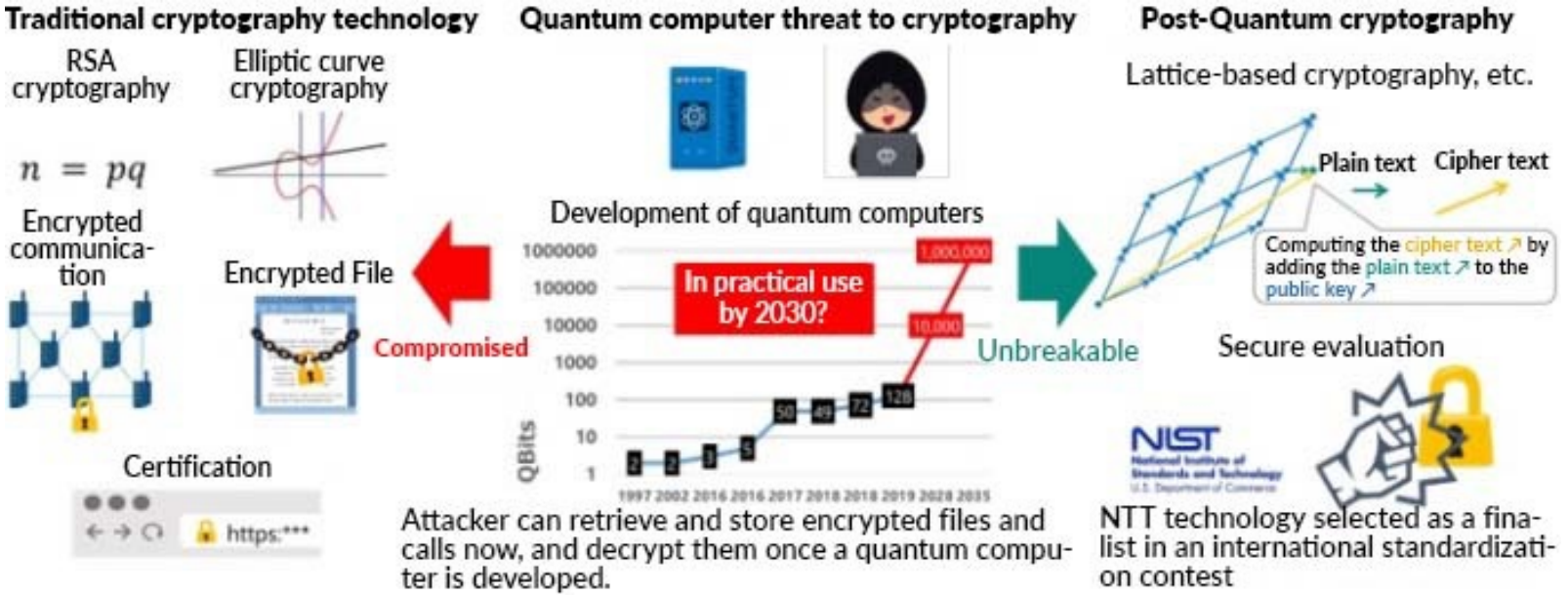
- **Conferences:**
  - **DEF CON / Black Hat:** The big "Hacker Summer Camp" in Vegas.
  - **BSides:** Local, community-driven, affordable.
  - **RSA:** Vendor-heavy, sales-focused.
- **Community:**
  - Twitter/X (Infosec Twitter) and LinkedIn are where the industry talks.
  - CTFs (Capture The Flag): Competitions to build skills.

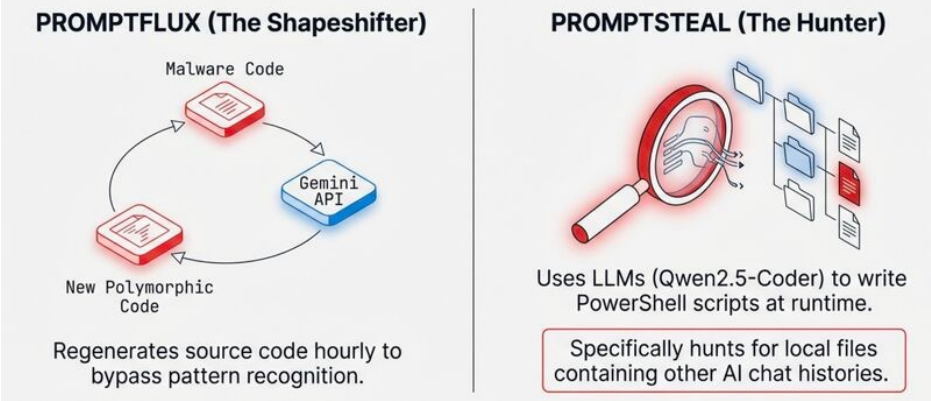
Ethics in Cybersecurity

- **The Hat Spectrum:**
  - **White Hat:** Ethical, authorized testing.
  - **Black Hat:** Criminal, malicious intent.
  - **Grey Hat:** "Scanning without permission," but good intent. (Still illegal).
- **Responsible Disclosure:**
  - The process of privately reporting a vulnerability to a vendor so they can fix it before the public knows.
- **CFAA:** The Computer Fraud and Abuse Act. (Don't scan what you don't own!).

Future Trends

- **AI & Automation:**
  - Attackers using AI to write better phishing emails.
  - Defenders using AI to triage alerts faster.
- **Post-Quantum Cryptography:**
  - Preparing for the day quantum computers break RSA encryption.
- **Privacy Engineering:**
  - "Privacy by Design" becoming a standard engineering requirement.





Competency Wrap-Up

- **Session 1:** Strategy (Pareto Principle).
- **Session 2:** Identity Security (Zero Trust).
- **Session 3:** Infrastructure Security (Visibility).
- **Session 4:** Governance, Risk, and Compliance (Translation).
- **Session 5:** Appicalition Security (Shift Left).
- **Session 6:** Incident Response (Resilience).
- **Session 7:** People (Culture).

Summary and Key Takeaways

- **Security is a Journey:** You are never "done."
- **Business Enabler:** Your job is to help the company sell safely, not to stop the company from selling.
- **Stay Curious:** The technology changes every year; the mindset remains the same.

End of the Lecture

Please do not hesitate to ask any questions to free your curiosity,

If you have any further questions after the class, please contact me via email (charnon@cmkl.ac.th).